Marsh

Liability Claims Bulletin: Cyber Edition

January 2022

Contents

Disclaimer: Claim outcomes are subject to facts and circumstances of each Claim, and subject to Policy terms and conditions, hence should not be used as a precedent.

Introduction

Cyber incidents have been on the rise in the recent years, and the trend has accelerated since the inception of the COVID-19 pandemic.

The rising cyber threats across industries and sectors has impacted the global insurance market, in terms of hardening premium rates and limited capacities, as insurers have opted to limit their liabilities by restricting coverages.

The first edition of our Liability Claims Bulletin highlighted how the evolving spectrum of risks and trends has led to an increase in the frequency and the number of disputes, and how managing these disputes are becoming a complex affair across different products and lines of business.

We are pleased to share the second edition of the Liability Claims Bulletin, which focuses on Cyber Claims.

James R. Clapper, Director of National Intelligence, in Worldwide Cyber Threats Testimony, Sept. 10, 2015, has said, "[T]he cyber threat cannot be eliminated; rather, cyber risk must be managed."

In this edition, we also intend to highlight our experiences in successfully managing some of the major cyber claims in the current year.

While the challenges in the settlement of such claims have been diverse, some of the common concerns across are:

- Engagement of specialists (incident response, forensic, public relations, credit monitoring etc.)
- Cost metrics and ceilings allowed by insurers
- Application of laws across jurisdictions
- Non-submission or delayed submission of essential documents
- No trigger of insuring clause
- Settlement without consent
- Breach of conditions/condition precedents
- Business interruption calculation

The Marsh Claims Practice has a philosophy to provide holistic support for clients' claims, identify trends and think strategically to achieve optimal claims outcomes today, tomorrow and in the long term.

Our bulletin focuses on how things can be done differently to avoid some of these challenges in the future. The *"Learnings for the Insureds"* section will let readers know what to do, and what not to do in the event of a claim.

Cyber and Data Security Claim Scenarios

1. Ransomware

Insured	An Indian global information technology company
Background	• Insured experienced a ransomware attack when their servers were affected and workstations became non-functional. • A ransom demand of around USD 800,000 was received. • The backups were not affected and the insured was able to restore its systems and return to operations in a clean environment. • No ransom was paid.
Claim amount	Forensic & Breach Counsel Costs: Around USD 500,000.
Policy type	Cyber
Challenges raised by insurers	Forensic expert and legal counsel engaged without the insurer's prior written consent.
Marsh's contribution	• We engaged with the forensic experts and the insured to make sure timely updates were shared with the insurers. • We explained to the insurers the necessity to engage experts in the absence of their prior consent.
Claim outcome	Full forensic costs over USD 500,000 were recovered (net off deductible).
Key learnings	• Do not engage forensic experts and/or breach counsels without the insurer's prior written consent. • Keep the insurers informed of all developments.

2. Malware/Ransomware

Insured	An Indian global information technology company
Background	• Insured became aware of a malware (ransomware) attack when some users experienced inaccessibility of their database files. • The impacted applications were shut down immediately to avoid any further spread, but there was a threat of code, data, and customization being lost. • The world's leading Forensics and Cyber security firms were engaged. • No ransom was paid.
Claim amount	Around USD 120,000.
Policy type	Cyber
Challenges raised by insurers	• Duplication of work done by the multiple vendors engaged to be discounted from the overall claim. • Retainer costs are not covered.
Marsh's contribution	With the help of the insured, we justified the engagement of multiple forensic/IT experts and how their roles were distinct and involved no duplication of work.
Claim outcome	Forensic costs around USD 108,000 subject to some deductions.
Key learnings	• Duplication of work done by vendors/forensic experts should be avoided. • Costs incurred under the retainer agreement are not payable – suggest a separate engagement/scope of work specific to the incident to be made outside of the retainers.

3. Phishing Attack

Insured	An Indian global information technology company
Background	Insured noted suspicious activity on their network regarding certain employee accounts, which were subjected to a sophisticated phishing campaign.
Claim amount	Forensic & Breach counsel costs: Around USD 3 Million.
Policy type	Cyber
Challenges raised by insurers	• Multiple forensic experts/ IT experts were engaged by the insured. • Experts engaged without the insurer's prior written consent.
Marsh's contribution	• As costs were reasonable and engagement of experts was an urgent requirement, we were successful in getting the vendor costs covered despite the initial challenges. • We challenged the insurer to cover some of the costs, which the insurer believed were not forensic/betterment costs.
Claim outcome	Forensic Costs and Breach Counsel costs: Around USD 1 Million. (net off deductible)
Key learnings	• Try to engage experts (forensic/legal) who are already empanelled with the insurer. Any engagement outside the panel should be with the insurer's prior written consent. • The cyber policy does not cover costs, which are incurred to update, upgrade, enhance or replace any computer system to a level beyond that which existed prior to the incident. It usually covers costs related to reinstatement.

4. Ransomware

Insured	An Indian multinational food service company
Background	• Insured became aware of a cyber-incident, where a Threat Actor compromised their user account, along with their confidential customer data. • Threat Actor demanded payment in Bitcoins. • Ransom was not paid.
Claim amount	Forensic & Breach Counsel Costs: Around USD 68,000.
Policy type	Cyber
Challenges raised by insurers	• According to the insurer, the data compromised was not Sensitive Personal Data/Information and the breach was not in violation of Data Protection Law. • Challenges raised regarding the legality of payment in Bitcoins.
Marsh's contribution	• We convinced the Insurer that the Threat Actor had successfully compromised the insured's systems and that there was a confirmed cyber-attack/data breach/privacy breach. • Assisted insured to notify CERT–IN, a Nodal Agency under the Information Technology Act, 2000. • We overcame the challenge of covering Bitcoin payments under the policy.
Claim outcome	Forensic & Breach Counsel Costs: Around USD 60,000 (net off deductible).
Key learnings	• Consult your broker before taking any action in the event of a claim. • Engaging with the insurer's panel of forensic experts helps. • Notify CERT-In as required under the Indian Information Technology Act, 2000. CERT-in may direct to inform the cyber cell. • Any exposures in other jurisdictions (US/UK etc.) would also require compliance of regulatory requirements as well as contractual requirements. Legal advice should be taken immediately.

5. Malware attack

Insured	An Indian global information technology company
Background	• Insured had a breach incident in the form of malware activity on their website. • Forensic experts were appointed with the insurer's prior written approval. • Insured filed a first-party claim seeking coverage for the forensic costs.
Claim amount	Forensic costs of around USD 126,000.
Policy type	Cyber
Challenges raised by insurers	• The insurer demanded that the insured prove the incident falls within either of the three categories, namely: - theft of data, - loss of data, or - denial of access. • In the absence of a third-party claim, a question was raised if the insuring clause under the policy triggers.
Marsh's contribution	We were able to convince the insurer that the first-party claim for recovery of forensic costs was independent of a third-party claim and policy responds to it.
Claim outcome	Full forensic costs around USD 68,000 (net off deductible)
Key learnings	• Keep the broker informed of developments at all stages and engage with the insurer immediately. • What is covered and what is not should be discussed with the broker as well as the insurer. • Cyber policies cover first-party forensic costs irrespective of a third-party claim.

6. Ransomware

Insured	A multinational Indian pharmaceutical company
Background	Insured faced a ransomware-attack on its computer systems. Subsequently, the plants and critical systems of the insured were also impacted leading to critical data loss.
Claim amount	Forensic costs of around USD 95,000. Separate Business Interruption costs claimed.
Policy type	Cyber
Challenges raised by insurers	• Complete documentation and information not provided. • Multiple forensic experts were involved.
Marsh's contribution	• We were able to help the insured provide all the necessary details/ information required by the insurer. • We were successful in convincing the insurers of the need for multiple forensic experts, i.e. each had a unique function and there was no duplication of work.
Claim outcome	The insurer agreed to pay full forensic costs. Calculation of business interruption loss is still being discussed with the insurer.
Key learnings	• Share the information - all reports provided by forensic experts / legal counsel with the insurer without any delay. • Cyber policies typically cover costs related to incident response, mitigation and reinstatement. Business Interruption losses require detailed and substantiated computations by the Insured. While the Insurer engages a Loss Adjuster, Marsh's in-house team of Forensic Accounting experts assists Insureds with their Business Interruption claims.

Summary of Key Learnings

1. Notify the details of the cyberattack to the insurer through your broker at the earliest. Any delay should be avoided.
2. Share all the relevant information about the claim with your broker as well as the insurers promptly.
3. Do not engage legal counsel/ forensic experts or incur any costs without the prior written approval of the insurer. Try to engage experts who are on the insurer's panel.
4. Do not engage multiple counsel/experts on a single claim. If it is unavoidable, the same should be done with the insurer's prior written consent.
5. Notify CERT-In as required under the Indian Information Technology Act, 2000, or other regulatory agencies as per the requirements in the impacted jurisdictions.
6. Have a thorough understanding of coverages, conditions and exclusions within your policy. Engage with your broker for a better understanding of policy wordings.

General Dos and Don'ts:

1. Inform the insurers as soon as the claim/circumstance comes to the company's notice. DO NOT delay reporting the claim.
2. Co-operate with the insurer. Provide regular updates on claims and prompt responses to insurers' queries.
3. Take all steps to minimize the loss and act as if you are uninsured.
4. Take appropriate action to preserve the insurer's right to recovery.
5. Engage with the forensics experts and take post–incident steps to harden company's cybersecurity.
6. DO NOT pay the ransom, admit liability for any accident or loss, or enter into any settlement with a third-party, without the consent of the insurer.
7. DO NOT incur legal expenses, which you expect to recover from insurers without first seeking their written consent.
8. DO NOT tell claimants that you are notifying insurers – "deep pocket" syndrome.

Know your team:

LEADERSHIP

ANUP DHINGRA

Managing Director, FINPRO & PEMA
Marsh India

+91 993 099 1978

anup.dhingra@marsh.com

BHISHMA MAHESHWARI

Senior Vice President, FINPRO - Marsh India

+91 704 592 2460

bhishma.maheshwari@marsh.com

Claims Solutions & Advisory

ALEX ROSATI

Head of FINPRO Claims - Marsh Asia

+852 628 36251

alexander.rosati@marsh.com

SIDHARTHA PATTNAIK

Head of Claims, Marsh India

+91 750 670 6162

sidhartha.pattnaik@marsh.com

AKSHARA SHARMA

Assistant Vice President, FINPRO - Marsh India

+91 915 202 0460

akshara.sharma@marsh.com

KAUSTUV DAS

Manager, FINPRO - Marsh India

+91 897 671 0987

kaustuv.das@marsh.com

ARPITA CUDDAPAH

Manager, FINPRO - Marsh India

+91 865 799 1771

arpita.cuddapah@marsh.com

RADHIKA NIPHADKAR

Management Trainee, FINPRO - Marsh India

+91 865 796 2995

radhika.niphadkar@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $18 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.

Marsh India Insurance Brokers Pvt. Ltd. having corporate and the registered office at 1201-02, Tower 2, One World Center, Plot-841, Jupiter Textile Compound Mills, Senapati Bapat Marg, Elphinstone Road (W), Mumbai 400 013 is registered as a composite broker with Insurance and Regulatory Development Authority of India (IRDAI). Its license no. is 120 and is valid from 03/03/2021 to 02/03/2024. CIN: U66010MH2002PTC138276.